

REMARKS

The Examiner rejected Claim 1 under 35 U.S.C. 102(b) as being anticipated by Scholer. Applicant traverses this rejection.

Regarding Claim 1, the Examiner stated that Scholer discloses the forwarding of keys using a security station service, where a second processor sends a key to a third processor as shown in the passage at col. 2, line 34-42. The Examiner goes on to state that the third processor forwards the key to the first processor and the first processor sends a message using the key as shown at col. 2, line 60-65 and col. 6, lines 20-38.

First, Applicant must point out that the claim requires the first processor to send a message using the key to the second data processor, not just send a message using the key.

Second, the Examiner does not explicitly state which of the many keys in Scholer corresponds to the key in question.

Scholer teaches that processor 4 sends a message containing a key, K, for an encryption system to the Security Station (SSS) using a public key system A. Hence, Applicant submits that Terminal 4 in Scholer must correspond to the second data processor of Claim 1, and terminal 8, i.e., SSS 8, must correspond to the third terminal of the claim. This leaves terminal 6 to fill the function of the first terminal recited in the claim. Scholer teaches that K is sent as part of a message that is encrypted using public key system A. The secret part of system A is held in terminal 4 and SSS has the public key part, PK.A. Hence, the first encryption protocol must be the code system using K, and the second encryption protocol is A to satisfy the claim.

SSS, i.e., the third data processor of the claim, forwards K to terminal 6, i.e., the first data processor, in the RCPT message sent by SSS to terminals 4 and 6 using a public key system N. The first data processor decrypts the RCPT message and extracts K, which it uses to decrypt <MSG>K, and hence, receive the message from the second data processor.

The problem with the Examiner's assignments lies in the fact that there is no teaching of terminal 6 sending a message to terminal 4 using key K. In the system taught in Scholer, the process ends with terminal 6 having received and decrypted the message from terminal 4 and terminal 4 having received the receipt message. The purpose of the scheme taught in Scholer is to deliver a message with a return receipt to a specified terminal, not to provide a conversation between the terminals once the message is sent. Accordingly, Applicant submits that Scholer does not anticipate Claim 1 or the claims dependent therefrom.

With reference to Claim 2, the Examiner stated that Scholer discloses that the first processor has insufficient computational resources to execute the second encryption protocol. The Examiner points to 4B, items 8, & 63. Applicant must disagree with the Examiner's reading of Scholer. First, Figure 4B is a block diagram of the security service station 8. As noted above, SSS 8 is the third processor. Second, the second encryption protocol is the public key encryption protocol A. SSS 8 must have the required computational resources since it decrypts the message from terminal 4 sent with that protocol. Furthermore, it should be noted that all of the terminals in Scholer have the computational resources to encrypt and decrypt messages in the public key system, since each one performs such encryptions and decryptions during the execution of the algorithm that is taught in Scholer. The only terminal that might lack the computational capacity to execute one of the code systems is SSS 8, which never decrypts <MSG>.K. It should be noted that terminals 4 and 6 encrypt and decrypt messages in the code system based on K. SSS 8 is never required to decrypt <MSG>.K, SSS 8 is not required to have the computational resources for that code system. However, there is no teaching that SSS 8 lacks the resources in question. The mere fact that some result might be true is not sufficient to sustain a rejection for anticipation. Hence, Applicant submits that there are additional grounds for allowing Claim 2.

With respect to Claim 4, the Examiner maintains that the passage at column 5, lines 32-42 teaches that the key is sent in response to a message from the first processor to the second processor. As noted above, the key is sent in response to a message from terminal 4 (the third data processor) to terminal 6 (the first data processor). There is no teaching of a message being sent from terminal 6 to terminal 4. Accordingly, there are additional grounds for allowing Claim 4.

Regarding Claims 5 and 6, the Examiner stated that Scholer discloses the internet and LAN in a passage at col. 6, lines 56-66 and in Fig. 1. Applicant must disagree with the Examiner's reading of this passage in Scholer. The cited passage does not mention the internet or a LAN. Claim 5 requires that the network segment connecting the second and third data processors, i.e., the communication network connecting terminal 4 and terminal 8 be the internet. Applicant can find no such teaching at the cited passage or anywhere else in the reference. Similarly, Applicant can find no mention of a local area network connecting terminals 4 and 8 in Scholer. Scholer merely refers to a set of terminals that are connected by a communication network. Accordingly, there are additional grounds for allowing Claims 7 and 8.

Regarding Claims 7-8, the Examiner stated that Scholer teaches these features in the passage at col. 5, lines 25-28 and in Fig. 2. Applicant must disagree with the Examiner's reading of the reference. Claim 7 requires the network segment between the first and third data processors to have a higher level of security than the insecure network segment that connects the second and third data processors. The cited passage does not teach anything about the relative security of the various segments. Furthermore, Applicant can find no mention of the relative security of the segments anywhere in Scholer. Hence, there are additional grounds for allowing Claim 7.

With reference to Claim 8, as noted above, the first encryption protocol must be the one using key, K, and the second encryption protocol is the public key protocol. The Examiner has not pointed to any teaching in Scholer that the encryption system based on K requires less computational resources than the public key encryption system. Hence, there are additional grounds for allowing Claim 8.

I hereby certify that this paper is being sent by FAX to 571-273-8300.

Respectfully Submitted,



Calvin B. Ward
Registration No. 30,896
Date: Jan. 23, 2006

Agilent Technologies, Inc.
Legal Department, M/S DL429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599
Telephone (925) 855-0413
Telefax (925) 855-9214